BENNET & BENNET PLLC

**Law Offices of Bennet & Bennet, PLLC**

*Maryland*
4350 East West Highway, Suite 201
Bethesda, Maryland 20814
Tel: (202) 371-1500
Fax: (202) 371-1558
www.bennetlaw.com

*District of Columbia*
10 G Street NE, Suite 710
Washington, DC, 20002

**Caressa D. Bennet**
**Michael R. Bennet**
**Gregory W. Whiteaker**
**Marjorie G. Spivak***
**Donald L. Herman, Jr.**
**Kenneth C. Johnson‡**
**Howard S. Shapiro**
**Daryl A. Zakov**
**Robert A. Silverman**
**Anthony K. Veach#**

***Of Counsel***
**Andrew Brown**

*Admitted in DC & PA Only
‡Admitted in DC & VA Only
Admitted in DC & WA Only
Admitted in DC & ME Only
#Admitted in DC & FL Only

January 28, 2011

**Via ECFS**

Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, S.W., Suite TW-A325
Washington, DC 20554

**Re: CPNI Certification and Accompanying Statement**
**EB Docket No. 06-36**

Dear Ms. Dortch:

TMP Corporation dba Simmetry Wireless ("the Company"), by its attorneys and pursuant to Section 64.2009(e) of the Commission's Rules, hereby submits its annual Customer Proprietary Network Information (CPNI) certification and accompanying statement.

Should you have any questions or need further information, please contact the undersigned.

Sincerely,

/s/

Marjorie Spivak

cc: Best Copy and Printing, Inc.
Attachments

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification EB Docket 06-36**

Annual 64.2009(e) CPNI Certification covering the prior calendar year 2010

1. Date filed: January 28, 2011

2. Name of company(s) covered by this certification: TMP Corporation d/b/a Simmetry Wireless

3. Form 499 Filer ID: 821328

4. Name of signatory: James W. Broemmer, Jr.

5. Title of signatory: President

6. Certification:

I, James W. Broemmer, Jr., certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.,* proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company received one customer complaint in the past year concerning the unauthorized release of a customer's CPNI to an individual not authorized to receive the information. The company properly notified law enforcement of the breach by sending electronic notification through the central reporting facility to the United States Secret Services and the FBI and took disciplinary action against the employee responsible for the breach.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____
James W. Broemmer, Jr.

**Attachments:** Accompanying Statement explaining CPNI procedures

# CPNI Usage Policy Statement

Pursuant to Section 64.2009(e) of the Federal Communications Commission's rules, this statement explains how the operating procedures of TMP Corporation d/b/a Simmetry Wireless (the "Company") ensure compliance with Part 64, Subpart U, of the FCC's rules.

## Company's Usage of CPNI

The Company has CPNI Procedures that set forth the Company's CPNI policies and outline what CPNI is and when it may or may not be used without customer approval by the Company.

The Company's Procedures set forth that the use of CPNI for the purpose of marketing a service to which a customer does not already subscribe is prohibited without prior customer notice and approval. The Company will not provide to any affiliate, CPNI of any customer who does not also subscribe to the services provided by that affiliate, without prior customer notice and approval.

The Company does not release CPNI to third parties without an affirmative written request from the subscriber.

## The Company's Notice and Approval Procedures

The Company's Procedures set forth the manner in which the Company obtains approval from customers for the use of CPNI for Company to notify subscribers of new communications-related services it may offer. The Company's procedures set forth whether such approval must be obtained through written, oral or electronic methods. The Company's Procedures set forth the period of time when such approval or disapproval to use CPNI remains in effect and the point in time when such approval is limited or revoked.

The Company's Procedures require that the Company maintain records of customer approval, whether oral, written or electronic, for at least one year.

The Company's Procedures set forth the procedures required to provide notification to customers prior to any solicitation for customer approval of the Company's right to use a customer's CPNI. Such procedures require the Company to provide a "Notice" to a customer explaining that the customer has a right, and the Company has a duty, under federal law to protect the confidentiality of CPNI. The Notice must explain to the customer that the customer may restrict the use of, disclosure of, and access to its CPNI. The Company maintains records of all such notifications for at least one year.

The Company's Procedures require that any customer notification provide information sufficient to enable a customer to make an informed decision as to whether to permit the Company to use its CPNI. At a minimum, such notification must include a description of the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses and deny or withdraw access to the CPNI at any time. The notification must advise the customer of the precise steps the customer must take to grant or deny access to CPNI, and state that a denial of approval will not affect the provision of any services to which the customer subscribes. The Company's notification must be proximate to any solicitation for the use of CPNI.

The Company's CPNI Procedures set forth the use of Opt-out customer approvals, and outline FCC requirements regarding methods of delivery, timing of response and content requirements.

**Company's CPNI Safeguards**

The Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

The Company has established procedures for the training of its personnel. Employees have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Procedures describe the disciplinary process related to noncompliance with CPNI obligations. Refresher training courses are often scheduled.

The Company's CPNI Procedures contain express disciplinary procedures applicable to employees who violate Company policies, including CPNI policies, which can include termination of employment.

The Company maintains a written record of its sales and marketing campaigns that use CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, the date and purpose of the campaign, and the specific products and services offered as part of the campaign. The Company maintains these records for a period of at least one year.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules. The Company's supervisory process ensures compliance with the FCC's rules on outbound marketing situations, and the Company maintains records of compliance with these rules for a period of at least one year. The Company's procedures require that all sales personnel obtain supervisory approval of any proposed outbound marketing request.

The Company has appointed a corporate officer that has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting such certification and accompanying statement of how the company complies with the FCC's CPNI rules to the FCC by March 1.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

The Company only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, the Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without the Company's assistance, then the Company is permitted to discuss the call detail information provided by the customer.

The Company has established a system of passwords and password protection. For accounts that are password protected, the Company cannot obtain the password by asking for readily available

biographical information or account information to prompt the customer for his password. A customer may also access call detail information by establishing an online account or by visiting a carrier's retail location. If a password is forgotten or lost, the Company calls the customer at the phone number of record or sends the information to the address of record.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

If a customer is able to provide to the Company, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call) then the Company proceeds with its routine customer carrier procedures. Under these circumstances, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

The Company password-protects online access to all CPNI, call detail and non-call detail. The Company may provide customers with access to CPNI at a Company retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

The Company notifies a customer immediately when a password, backup for a forgotten password, online account, or address of record is created or changed through a Company-originated voicemail or text message to the telephone number of record, or by mail to the address of record.

In the event of a CPNI breach, the Company delays customer notification of breaches until law enforcement has been notified of a CPNI breach. The Company will notify law enforcement of a breach of its customers' CPNI within seven business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct the Company not to disclose the breach for an initial 30-day period. The law enforcement agency must provide in writing to the carrier its initial direction and any subsequent direction. The Company, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if the Company believes there is an extraordinarily urgent need to notify a customer or class of customers to avoid immediate and irreparable harm.

The Company maintains a record of any discovered breaches and notifications to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two year.

**Actions Taken Against Data Brokers and Customer Complaints**

The Company took no actions against data brokers during the previous calendar year. The company received one customer complaint in the past year concerning the unauthorized release of a customer's CPNI to an individual not authorized to receive the information. The company properly notified law

enforcement of the breach by sending electronic notification through the central reporting facility to the United States Secret Services and the FBI and took disciplinary action against the employee responsible for the breach.